BANK INDONESIA

Unofficial Translation

BANK INDONESIA REGULATION
NUMBER 14/3/PBI/2012
CONCERNING
THE ANTI-MONEY LAUNDERING
AND PREVENTION OF TERRORISM FINANCING PROGRAMME
FOR PAYMENT SYSTEM SERVICE PROVIDERS OTHER THAN BANKS

BY THE GRACE OF GOD THE ALMIGHTY
THE GOVERNOR OF BANK INDONESIA,

Considering:

a. whereas provision of payment system services by providers other than banks has undergone expansion both in numbers of providers and in volume and nominal value of transactions;
b. whereas to prevent the exploitation of provision of non-bank payment system services for money laundering and terrorism financing, it is necessary to implement an anti-money laundering and prevention of terrorism financing programme for payment system service providers other than banks;
c. whereas the anti-money laundering and prevention of terrorism financing programme for payment system service providers other than banks needs to be guided by generally accepted international principles;
d. now therefore, based on the considerations referred to in letter a, letter b and letter c, it is necessary to enact a Bank Indonesia Regulation concerning the Anti-Money Laundering and Prevention of Terrorism Financing

Programme…

Programme for Payment System Service Providers Other Than Banks;

In view of:

1. Act Number 23 of 1999 concerning Bank Indonesia (State Gazette of the Republic of Indonesia Number 66 of 1999, Supplement to the State Gazette Number 3843), as last amended by Act Number 6 of 2009 concerning Adoption of Government Regulation in Lieu of Act of Parliament Number 2 of 2008 concerning the Second Amendment to Act Number 23 of 1999 concerning Bank Indonesia as Act of Parliament (State Gazette of the Republic of Indonesia Number 7 of 2009, Supplement to the State Gazette of the Republic of Indonesia Number 4962);
2. Act Number 15 of 2003 concerning Adoption of Government Regulation in Lieu of Act of Parliament Number 1 of 2002 concerning Eradication of Terrorism Financing as Act of Parliament (State Gazette of the Republic of Indonesia Number 45 of 2003, Supplement to the State Gazette of the Republic of Indonesia Number 4284);
3. Act Number 8 of 2010 concerning Prevention and Eradication of Money Laundering (State Gazette of the Republic of Indonesia Number 122 of 2010, Supplement to the State Gazette of the Republic of Indonesia Number 5164);
4. Act Number 3 of 2011 concerning Funds Transfers (State Gazette of the Republic of Indonesia Number 39 of 2011,

Supplement to the State Gazette of the Republic of Indonesia Number 5204);

HAS DECREED:

To enact: THE BANK INDONESIA REGULATION CONCERNING THE ANTI-MONEY LAUNDERING AND PREVENTION OF TERRORISM FINANCING PROGRAMME FOR PAYMENT SYSTEM SERVICE PROVIDERS OTHER THAN BANKS.

## CHAPTER I
## GENERAL PROVISIONS
### Article 1

The terminology used in this Bank Indonesia Regulation has the following meanings:

1. "Bank" is a Commercial Bank as defined in Act Number 7 of 1992 concerning Banking as amended by Act Number 10 of 1998 and Act Number 21 of 2008 concerning Sharia Banking.
2. "Payment System Service Provider Other Than Bank," hereafter referred to as Provider, is a business entity incorporated under the laws of Indonesia that has obtained a licence from Bank Indonesia to provide payment system services.
3. "Card-Based Payment Instrument," hereafter referred to as CBPI, is a payment instrument as referred to in the Bank Indonesia Regulation governing card-based payment instruments.
4. "Electronic Money," hereafter referred to as Electronic Money, is a payment instrument as referred to in the Bank Indonesia Regulation governing electronic money.

5."Remittance …

5. "Remittance Services," hereafter abbreviated as RS, is the business of remittances or funds transfers as referred to in the Bank Indonesia Regulation governing the business of remittances or funds transfers.
6. "Service Users" are parties using the services of Providers.
7. "Money Laundering" is money laundering as referred to in the Act governing the prevention and eradication of money laundering.
8. "Terrorism Financing" is the use of wealth, whether directly or indirectly, for terrorism activities as referred to in the Act governing eradication of terrorism.
9. "Customer Due Diligence," hereafter abbreviated as CDD, comprises the activities of identification, verification and monitoring performed by a Provider to ensure that the transaction involved is appropriate to the profile of the Service User.
10. "Enhanced Due Diligence," hereafter abbreviated as EDD, is a more in-depth CDD performed by a Provider when contacted by a Service User categorised as high risk, including a Politically Exposed Person, in regard to the possibility of money laundering and terrorism financing.
11. "Beneficial Owner" is any natural person who holds funds, controls the transactions of a Service User, issues authorisation for a transaction to take place and/or exercises control through a legal entity or under an agreement.
12. "Politically Exposed Person," hereafter abbreviated as PEP, is any person entrusted to hold public office, including bearer of state office as referred to in the laws and regulations governing bearers of state office, and/or person registered as a member of a political party exercising influence on the policies and operations of the political party, whether of Indonesian nationality or foreign nationality.
13. "Suspicious Transaction" is a suspicious financial transaction as referred to in the Act governing the prevention and eradication of money laundering.

14. "Financial Transaction Analysis and Reporting Centre," hereafter abbreviated as PPATK, is PPATK as referred to in the Act governing the prevention and eradication of money laundering.
15. "Anti-Money Laundering and Prevention of Terrorism Financing," hereafter abbreviated at AML and PTF, are efforts to prevent and eradicate money laundering and financing of terrorism.

## CHAPTER II
## SCOPE OF OPERATORS AND THE AML AND PTF PROGRAMME

### Article 2

(1) Providers are required to implement the AML and PTF programme.
(2) Providers as referred to in paragraph (1) encompass:
    a. issuers and/or acquirers in CBPI activities;
    b. issuers and/or acquirers in Electronic Money activities; and/or
    c. RS providers.

### Article 3

(1) Implementation of the AML and PTF programme as referred to in Article 2 paragraph (1) shall encompass at least the following:
    a. responsibilities of the Board of Directors and active oversight by the Board of Commissioners;
    b. written policy and procedures;
    c. internal control; and
    d. human resources.
(2) In implementing the AML and PTF programme as referred to in paragraph (1), a Provider must be guided by the provisions of this Bank Indonesia Regulation.

CHAPTER III

RESPONSIBILITIES OF THE BOARD OF DIRECTORS
AND ACTIVE OVERSIGHT BY THE BOARD OF COMMISSIONERS

Article 4

The responsibilities of the Board of Directors of a Provider as referred to in Article 3 paragraph (1) letter a encompass at least the following:

a. establishment of written policy and procedures for implementation of the AML and PTF programme based on approval by the Board of Commissioners;
b. ensure that the AML and PTF programme is implemented in accordance with the established written policy and procedures;
c. ensure that the written policy and procedures for the AML and PTF programme are in line with changes and developments in products, services, technology, modus of Money Laundering or Terrorism Financing and the applicable provisions pertaining to the AML and PTF programme;
d. ensure the submission of Suspicious Transaction reports, cash transaction reports and incoming and outgoing foreign transactions to PPATK in accordance with laws and regulations;
e. ensure that all employees are equipped with knowledge and/or training on implementation of the AML and PTF programme; and
f. ensure the updating of customer profiles and customer transaction profiles.

Article 5

Active oversight by the Board of Commissioners of a Provider as referred to in Article 3 paragraph (1) letter a shall encompass at least the following:

a. issue approval for the policy for implementation of the AML and PTF programme; and

b. monitor performance of the Board of Directors responsibilities for implementation of the AML and PTF programme.

## CHAPTER IV
## POLICY AND PROCEDURES

### Article 6

(1) The written policy and procedures as referred to in Article 3 paragraph (1) letter b shall encompass at least the following:
   a. performance of CDD and EDD;
   b. document administration;
   c. establishment of Service User profiles and updating of Service User information;
   d. refusal and discontinuation of business dealings;
   e. policy and procedures for funds transfers; and
   f. reporting to PPATK;

(2) The Provider is required to convey the written policy and procedure as referred to in paragraph (1) and any amendment thereto to Bank Indonesia.

(3) A Provider that has a branch or subsidiary operating outside the territory of the unitary state of the Republic of Indonesia shall ensure that the branch or subsidiary complies at the minimum with the requirements for policy and procedures governing the AML and PTF program as stipulated in this Bank Indonesia Regulation.

### Part One
### Performance of CDD and EDD

Sub-Part 1

General Provisions

Article 7

(1) Providers are required to perform CDD or EDD on Service Users.

(2) Service Users as referred to in paragraph (1) include prospective Service Users.

(3) The obligation to perform CDD or EDD as referred to in paragraph (1) is waived in the case of provision of payment system services with low risk.

(4) In performing CDD or EDD as referred to in paragraph (1), Providers must apply a risk-based approach taking account of the characteristics of the payment system services to be performed and the profile of the Service User.

Sub-Part 2

Performance of CDD

Article 8

Providers are required to perform CDD when:

a. the Provider enters into business dealings with a Service user or prospective Service User;

b. there are doubts about the authenticity of identity information obtained from a Service User or prospective Service User.

Article 9

(1) When performing CDD for an individual Service User and/or prospective individual Service User, Providers are required to demand documents bearing information on:

a. identity of the Service User, stating at least the following:

1. full name including alias, if any;

2. number of identity document, substantiated by producing the document in question;
3. residential address stated on the identity card;
4. latest residential address including telephone number, if any;
5. place and date of birth;
6. nationality; and
7. gender;

b. value and date of the transaction; and

c. other information enabling the Provider to ascertain the profile of the Service User, if needed.

(2) Service Users conducting receipt transactions are exempted from demanding documents bearing information as referred to in paragraph (1) letter b.

Article 10

(1) When performing CDD for Service Users and/or prospective Service Users other than natural persons, the Provider is required to demand documents bearing information in regard to:

a. identity of the Service User, stating at least the following:
   1. name and incorporation of the Service User business entity;
   2. number of business licence issued by a competent agency;
   3. address of domicile of the Service User; and
   4. Taxpayer ID Number of the Service User.

b. identity of the natural person acting on behalf of and in the name of the Service User, using documents as referred to in Article 9 paragraph (1) letter a.

c. power of attorney or other legal document that assigns powers to a person as referred to in letter b to act on behalf of and in the name of the Service User;

d. value and date of the transaction; and

e. other information enabling the Provider to ascertain the profile of the Service User, if needed.

(2) Service Users conducting receipt transactions are exempted from demanding documents bearing information as referred to in paragraph (1) letter d.

Sub-Part 3

Performance of CDD by Third Parties

Article 11

(1) Providers may use the findings of CDD performed by a third party with regard to Service Users who are existing customers or consumers of the third party.

(2) CDD findings as referred to in paragraph (1) may be used by the Provider if the third party:

a. has a CDD procedure in accordance with the applicable provisions;

b. has a collaborative arrangement with the Provider in the form of a written agreement;

c. is willing to comply with requests for information and copies of supporting documents if needed by the Provider at any time for the purpose of implementing the AML and PTF programme; and

d. is domiciled in a country that has implemented the recommendations of the Financial Action Task Force (FATF).

(3) The Provider is required to perform identification and verification of the findings of any CDD performed by a third party as referred to in paragraph (1).

(4) A Provider using the findings of CDD from a third party as referred to in paragraph (1) bears responsibility to perform document administration as referred to in Article 22.

Sub-Part 4

Performance of EDD

Article 12

Providers are required to perform EDD of Service Users and/or prospective Service Users who:

a. are high risk, including PEPs;

b. are suspected of conducting suspicious activities pertaining to money laundering or terrorism financing; and/or

c. conduct transactions in the rupiah currency and/or a foreign currency in a value of at least or equivalent to Rp 100,000,000.00 (one hundred million rupiahs).

Article 13

(1) In performing EDD on individual Service Users and/or prospective individual Service Users, Providers are required to demand documents bearing information on the following:

a. identity of the Service User and prospective Service User, stating:

1. full name including alias, if any;
2. number of identity document, substantiated by producing the document in question;
3. residential address stated on the identity card;
4. latest residential address including telephone number, if any;
5. place and date of birth;
6. nationality; and
7. gender;

b. value and date of the transaction;

c. source of funds;

d. purpose of transaction; and

e. other information enabling the Provider to ascertain the profile of the Service User and/or prospective Service User, if needed

(2) Service Users conducting receipt transactions shall be exempted from demanding documents bearing information as referred to in paragraph (1) letter b until letter d.

(3) In addition to demanding documents as referred to in paragraph (1), the Provider is required to examine the plausibility of transactions performed by Service Users

Article 14

(1) When performing EDD for Service Users and prospective Service Users other than natural persons, Providers are required to demand documents bearing information on:

a. identity of the Service User and prospective Service User, containing the following:
   1. name and legal incorporation of the Service User;
   2. number of business licence issued by a competent agency;
   3. address of domicile of the Service User;
   4. place and date of establishment of the Service User; and
   5. Taxpayer Identity Number of the Service User.

b. identity of the Service User management;

c. identity of the natural person acting on behalf of and in the name of the Service User, using documents as referred to in Article 13 paragraph (1) letter a.

d. power of attorney or other legal document that assigns powers to a person as referred to in letter c to act on behalf of and in the name of the Service User;

e. transaction value and date;

f. source of funds;

g. purpose of the transaction; and

h. other information enabling the Provider to ascertain the profile of the Service User, if needed.

(2) Service Users conducting receipt transactions shall be exempted from demanding documents bearing information as referred to in paragraph (1) letter e until letter g.

(3) In addition to demanding documents as referred to in paragraph (1), the Provider is required to examine the plausibility of transactions performed by Service Users.

Article 15

Provision of services to high risk Service Users may operate only with approval from a senior officer of the Provider.

Article 16

In the event a Provider conducts a transaction with a Service User categorised as PEP or high risk, the Board of Directors of the Provider shall be directly responsible for implementation of the AML and PTF programme with regard to this Service User.

Sub-Part 5

Performance of Document Verification

Article 17

(1) Providers are required to obtain assurance of the true identity of Service Users and/or prospective Service Users.

(2) Providers are required to meet face to face with a prospective Service User and/or Service User who for the first time is using a payment system service

provided by the Provider in order to obtain assurance of the true identity of that prospective Service User and/or Service User.

Article 18

(1) The Provider is required to check for truthfulness and perform verification of supporting documents as referred to in Article 9, Article 10, Article 13 and Article 14 on the basis of official documents and/or other reliable sources of information and to confirm these documents as up to date data.

(2) The Provider may interview a Service User and/or prospective Service User to check and obtain assurance of the validity and truthfulness of documents as referred to in paragraph (1).

(3) In case of doubt, the Provider must ask the User and/or prospective Service User to provide more than one identity document issued by a competent authority to obtain assurance of the true identity of the Service User.

(4) The Provider is required to complete the identity verification process for the User and/or prospective Service User before providing payment system services to the Service User.

Sub-Part 6

Monitoring of Service User Transactions

Article 19

(1) Providers are required to maintain ongoing monitoring to ascertain the plausibility of transactions by Service Users with regard to the Service User profile.

(2) Providers are required to analyse all transactions lacking plausibility with regard to the Service User profile.

(3) Analysis as referred to in paragraph (2) must take account of transactions of high complexity, high value and in departure from customary habit, or without an economic interest.

Sub-Part 7

Beneficial Owners

Article 20

(1) Providers are required to ascertain whether a Service User or prospective Service User is acting to represent a Beneficial Owner in business dealings with the Provider.

(2) The Provider is required to perform the entire CDD or EDD procedure for a Beneficial Owner as would be performed for a Service User or prospective Service User.

(3) When performing CDD or EDD for a Beneficial Owner as referred to in paragraph (2), the Provider is required to demand from the Beneficial Owner identity documents as referred to in Article 9 paragraph (1) letter a or Article 13 paragraph (1) letter a.

(4) The truthfulness of information provided by the Beneficial Owner shall be verified in accordance with the provisions referred to in Article 17 and Article 18.

Article 21

The obligation for submission of identity documents and verification of the truthfulness of Beneficial Owner information for performance of CDD or EDD as referred to in Article 20 shall not apply to a Beneficial Owner representing a:

a. state/government institution; or

b. company listed on the stock exchange.

Part Two

Document Administration

Article 22

(1) Providers are required to maintain administration of:
   a. documents pertaining to information on Services Users, prospective Service Users and/or Beneficial Owners for a period of no less than 5 (five) years after conclusion of the transaction and/or provision of services to the Service User;
   b. financial documents pertaining to Service Users with a retention period as stipulated in the Laws governing company documents.

(2) In the event of a transaction meeting the criteria referred to in Article 19 paragraph (2) and paragraph (3), the Provider is required to maintain dedicated administration of transaction data and/or documents of the transactions for a period of 5 (five) years after the transaction is declared a transaction that meets the criteria referred to in Article 19 paragraph (2) and paragraph (3).

Article 23

Administration as referred to in Article 22 may be conducted over a longer period if related to a particular case and if requested by a competent authority, such as Bank Indonesia or PPATK.

Part Three

Determination of Profile and Updating of Information on Service Users

Article 24

(1) Providers are required to establish profiles of Service Users when performing CDD and EDD.

(2) Service User profiles as referred to in paragraph (1) must be based on adequate information concerning the Service User.

Article 25

(1) Providers are required to update information on Service Users.

(2) Updating of information as referred to in paragraph (1) shall be performed for all documents, data and information collected within the framework of CDD and/or EDD.

Part Four

Refusal and Discontinuation of Business Dealings

Article 26

Providers are required to refuse service to prospective Service Users who:

a. do not possess valid identity documents;

b. are unable to produce valid identification of their Beneficial Owner;

c. are unable to provide adequate information to put together a Service User profile; or

d. are suspected of using a false name or are unwilling to supply a name (anonymous).

Article 27

A Provider is required to discontinue business dealings with any Services User who fails to satisfy requirements pertaining to performance of CDD or EDD.

Part Five

Policy and Procedures for Funds Transfer

Article 28

In conducting funds transfer activities, Providers are required to obtain and ensure the completeness of information on the identity of the sending Service User.

Part Six

Reporting to PPATK

Article 29

(1) Providers are required to submit Suspicious Transaction reports, cash financial transaction reports and financial statements on incoming and outgoing foreign funds transfers as stipulated in the laws and regulations governing the prevention and eradication of money laundering.

(2) The obligation of a Provider to report Suspicious Transactions also applies to transaction suspected to be linked to terrorism activity or Financing of Terrorism.

(3) Submission of reports as referred to in paragraph (1) shall follow the guidance of provisions issued by PPATK.

CHAPTER V

INTERNAL CONTROLS

Article 30

(1) Providers are required to put together and implement internal controls.

(2) Internal controls as referred to in paragraph (1) shall, among others, be put in place by establishing a board of directors policy concerning:

a. limits on powers and responsibilities of units related to implementation of the AML and PTF programme; and

b. examinations by the internal audit function of the effectiveness of the AML and PTF programme implementation.

(3) The staff of the internal audit function of the Provider shall report to PPATK any Suspicious Transaction as referred to in Article 29 that is discovered when conducting an audit and not previously reported by the Provider.

## CHAPTER VI
## HUMAN RESOURCES

### Article 31

To prevent the exploitation of the Provider as a medium or destination of Money Laundering or Terrorism Financing involving internal parties, the Operator is required to implement a screening procedure for recruitment of new employees.

### Article 32

Providers are required to provide ongoing training concerning:

a. implementation of the laws and regulations pertaining to the AML and PTF programme;

b. techniques, methods and typology of Money Laundering or Terrorism Financing; and

c. policy and procedures for implementation of the AML and PTF programme and the roles and responsibilities of employees in eradication of Money Laundering and Terrorism Financing.

### Article 33

(1) Providers are required to establish a dedicated unit and/or appoint an officer of the Provider responsible for implementation of the AML and PTF programme.

(2) The dedicated unit and/or officer as referred to in paragraph (1) shall be responsible to the board of directors.

(3) The dedicated unit and/or officer as referred to in paragraph (1) must have adequate capacity and have authorisation to access all Services User data and other related information.

(4) If a Provider is unable to establish a dedicated unit and/or appoint an officer of the Provider responsible for implementation of the AML and PTF programme as referred to in paragraph (1), the function shall be performed by a member of the board of directors.

## CHAPTER VII
## PROHIBITION ON DISCLOSURE OF CONFIDENTIAL INFORMATION (TIPPING OFF)

### Article 34

(1) The Board of Commissioners, Board or Directors and/or employees of a Provider are prohibited from informing a Service User or other party in any manner, whether directly or indirectly, of a Suspicious Transaction report in preparation or submitted to PPATK, with respect to the relevant laws and regulations.

(2) The provisions concerning the prohibition referred to in paragraph (1) do not apply to disclosure of information to Bank Indonesia.

## CHAPTER VIII
## OVERSIGHT

### Article 35

Bank Indonesia shall oversee the implementation of the AML and PTF programmes by Providers.

CHAPTER IX

SANCTIONS

Article 36

(1) Any Provider late in submission of a report as referred to in Article 29 shall be liable to administrative sanctions comprising a financial penalty of Rp 50,000.00 (fifty thousand rupiahs) per day of delay per report.

(2) Any Provider failing to submit a report as referred to in paragraph (1) within 30 (thirty) days after the report submission deadline shall be liable to sanctions comprising a written warning and a financial penalty of Rp 3,000,000.00 (three million rupiahs).

Article 37

Any provider failing to comply with obligations as referred to in Article 2, Article 3, Article 6, Article 7, Article 8, Article 9, Article 10, Article 11, Article 12, Article 13, Article 14, Article 17, Article 18, Article 19, Article 20, Article 22, Article 24, Article 25, Article 26, Article 27, Article 28, Article 29, Article 30, Article 31, Article 32, Article 33 and Article 39 shall be liable to administrative sanctions comprising the following:

a. written warning;

b. suspension of business as Provider, whether in whole or in part;

c. cancellation of licence; and/or

d. revocation of licence.

Article 38

Bank Indonesia may revoke the business licence of an Operator on the basis of a recommendation by PPATK.

CHAPTER X

TRANSITIONAL PROVISIONS

Article 39

Providers that obtained licences from Bank Indonesia prior to the enactment of this Bank Indonesia Regulation are required to submit and implement written policy and procedures as referred to in Article 6 paragraph (2) no later than 3 (three) months after the enactment of this Bank Indonesia Regulation.

CHAPTER XI

CONCLUDING PROVISIONS

Article 40

Further provisions concerning the Anti-Money Laundering and Combating of Terrorism Financing Programmes for Payment System Service Providers Other Than Banks shall be stipulated in a Circular Letter of Bank Indonesia.

Article 41

This Bank Indonesia Regulation shall come into force on 8 June 2013.

For the public to be informed, it is ordered that this Bank Indonesia Regulation be promulgated in the State Gazette of the Republic of Indonesia.

Enacted in Jakarta

Dated 29 March 2012

THE GOVERNOR OF BANK INDONESIA

(signed)

DARMIN NASUTION

Legislated…

Legislated in Jakarta
Dated 29 March 2012

THE MINISTER OF LAW AND HUMAN RIGHTS
OF THE REPUBLIC OF INDONESIA

(signed)

AMIR SYAMSUDDIN

BANK INDONESIA

ELUCIDATION

TO

BANK INDONESIA REGULATION

NUMBER: 14/3/PBI/2012

CONCERNING

THE BANK INDONESIA REGULATION CONCERNING THE ANTI-MONEY LAUNDERING AND PREVENTION OF TERRORISM FINANCING PROGRAMME FOR PAYMENT SYSTEM SERVICE PROVIDERS OTHER THAN BANKS

I. GENERAL REVIEW

The launching of the Anti-Money Laundering and Prevention of Terrorism Financing (AML and PTF) programmes for providers of payment systems services is nothing new. If these providers of payment system services are commercial banks, they are fully subject to the Bank Indonesia regulations governing AML and PTF for commercial banks. Similarly, if these providers of payment system services are Rural Banks, they are fully subject to the Bank Indonesia regulations governing AML and PTF for Rural Banks. The stipulation of AML and PTF for Payment System Service Providers Other Than Banks is intended for providers of payment services that are not banks, whether commercial banks or Rural Banks. As applies in the non-discrimination principles customarily followed in payment systems, no differences apply in the implementation of AML and PTF, whether to bank or to payment system service providers other than banks.

In the provision of payment system services essentially involving transfer of funds and payment activities, there is enormous potential for these two activities to be exploited for Money Laundering activities and the use of these activities in Terrorism Financing. The increasing rapidity of payment system activities and growing numbers of non-bank parties involved as providers of payment system services has reinforced the urge to stipulate and improve the role and cooperation of providers in law enforcement for operation of the AML and PTF programme. To this end, prevention

From…

from the outset through in-depth identification of payment system service users is of enormous significance. The compliance of service users with a number of requirements before concluding a transaction and compliance with a number of steps that must be performed by a provider is extremely important to mitigate legal risk, operational risk and reputational risk. Payment System Service Providers Other Than Banks, such as issues or acquirers in the provision of Card-Based Payment Instruments (CBPI) or Electronic Money, and/or providers of Remittance Services or funds transfers, have an important role in performing these processes.

For providers of payment system services, implementation of the AML and PTF programme is guided by the international standards for prevention and eradication of money laundering and terrorism financing issued by the Financial Action Task Force (FATF) on Money Laundering as set out in the FATF 40+9 Recommendations/Special Recommendations. These recommendations also comprise the reference used by the international community in assessment of a nation's compliance with implementation of the anti-money laundering and prevention of terrorism financing programme.

The role of Bank Indonesia as a Supervisory and Regulatory Institution as referred to in Act No. 8 of 2010 concerning Prevention and Eradication of Money Laundering (the AML Law), namely to issue regulations, conduct supervision and/or impose sanctions for violation of the AML and PTF regulations, also has importance for enforcement of the AML and PTF programme. The issuance of provisions in this Bank Indonesia regulation forms part of the Bank Indonesia role as a Supervisory and Regulatory Institution.

This Bank Indonesia Regulation, among others, sets forth limits on the understanding of the providers, the scope of the AML and PTF programme, performance of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD), the requirements that must be fulfilled and the roles that must be performed by the management of the provider, reporting obligations, and includes imposition of administrative sanctions for failure to comply with obligations. Activities performed

to identify, verify and monitor documents and the service user activities constitute part of the key activities that must be performed by a provider, moreover if the service user is a high risk party.

The stipulations in this Bank Indonesia regulation are intended primarily for Payment System Service Providers Other Than Banks engaged in the activities of Card-Based Payment Instruments, Electronic Money and/or provision of Remittance Services or funds transfer activities as referred to in the AML Law. There is enormous future potential for development of these payment system service products. If in the future the competent authorities for AML and PTF issue policies and recognise the existence of new providers in payment system services, it is possible for the AML and PTF programme stipulated in this Bank Indonesia regulation to be applied to these new providers.

With effective implementation of the AML and PTF programme for providers of payment system services, it is expected that providers will be able to operate on a sound basis so that ultimately this will bring overall improvement in security and efficiency in maintaining the payment system.

II. ARTICLE BY ARTICLE

Article 1

Self-explanatory

Article 2

Paragraph (1)

Self-explanatory.

Paragraph (2)

Letter a

"Issuer and/or acquirer in CBPI activities" is defined as an issuer and/or acquirer as stipulated in the Bank Indonesia Regulation governing CBPI.

Letter b

"Issuer and/or acquirer in Electronic Money activities" is defined as an issuer and/or acquirer as stipulated in the Bank Indonesia Regulation governing electronic money.

Letter c

"RS Provider" is defined as a Provider conducting Remittance Services or funds transfers as referred to in the Bank Indonesia Regulation governing RS or funds transfers.

Providers of CBPI and Electronic Money, other than issuers and/or acquirers, must support the implementation of AML and PTF programmes implemented by issuers and/or acquirers. Support by providers other than issuers and/or acquirers for AML and PTF programmes shall involve, among others, provision of data necessary to the implementation of AML and PTF programmes.

Article 3

Paragraph (1)

Letter a

"Board of Directors" is defined as follows:

a. for a Provider incorporated as a Limited Liability Company, the board of directors as referred to in the Act governing Limited Liability Companies;
b. for a Provider incorporated as a Regional Government Enterprise, the board of directors as referred to in the Act governing Regional Government Enterprises;

c. for a Provider incorporated as a Cooperative, the management as referred to in the Act governing Cooperatives;

d. for a Provider incorporated as a Public Enterprise, the board of directors as referred to in the Act governing State Owned Enterprises.

"Board of Commissioners" is defined as:

a. for a Provider incorporated as a Limited Liability Company, the board of commissioners as referred to in the Act governing Limited Liability Companies;

b. for a Provider incorporated as a Regional Government Enterprise, the board of commissioners as referred to in the Act governing Regional Government Enterprises

c. for a Provider incorporated as a Cooperative, the supervisory board as referred to in the Act governing Cooperatives;

d. for a Provider incorporated as a Public Enterprise, the supervisory board as referred to in the Act governing State Owned Enterprises.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Paragraph (2)

Self-explanatory.

Article 4

Self-explanatory.

Article 5…

Article 5

Self-explanatory.

Article 6

Paragraph (1)

Self-explanatory.

Paragraph (2)

Amendment to written policy and procedures that must be conveyed to Bank Indonesia means any significant amendment to the AML and PTF policy and procedures.

Paragraph (3)

Self-explanatory.

Article 7

Paragraph (1)

Self-explanatory.

Paragraph (2)

"Prospective Service User" is defined as a party indicating intent to use the services of a Provider.

Paragraph (3)

"Provision of payment system services with low risk" is the provision of payment system services with little potential for misuse, among others by reason of limited scope of use and value. Limited scope of use can be ascertained from the function of an instrument that may be used only for making payments. Limited value can be ascertained from a relatively low maximum limit on the amount of a payment instrument.

Examples …

Examples of payment system services with low risk include but are not limited to electronic money with a maximum value of Rp 1,000,000.- (one million rupiahs) that may not be used for funds transfers.

Paragraph (4)

The risk-based approach shall be guided by PPATK provisions, including but not limited to the grouping of Service Users by level of risk of possible money laundering or terrorism financing, based on levels of low, medium and high risk. Besides applying a risk-based approach, Providers must also pay attention to the characteristics of payment system services, such as value, volume and service users.

Aspects that may be considered by a Provider when establishing written policy and procedures for performance of CDD and EDD include but are not limited to the total number and value of transactions in the Service User profile (natural person, company or Beneficial Owner), line of business, geographical factors, frequency and value of transactions by the Service User.

Article 8

Self-explanatory.

Article 9

Paragraph (1)

Individual Service User is defined as a service user that is a natural person or individual, and not a business entity or legal entity.

Letter a

Identity document of the Service User includes but is not limited to identity card, driving licence, passport or other identity document bearing a photograph of the Service User.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Paragraph (2)

"Transaction of the nature of receipt" is defined as a transaction in which the Service User is the beneficiary of the transaction, including but not limited to receipt of a remittance transaction.

Article 10

Paragraph (1)

Service User other than a natural person is defined as a Service User from an institution, business entity or legal entity (legal person).

Letter a

Documents stating the name and incorporation of the Service User include but are not limited to deed of incorporation or articles of association of the Service User.

For Service Users comprising government/state institutions, it is sufficient for the documents to be presented to state the name and address of the government/state institution

Letter b

Self-explanatory.

Letter c

Other legal documents may comprise the articles of association or internal rules of a Service User that constitute the basis of power to represent the Service User

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Paragraph (2)

"Transaction of the nature of receipt" is defined as a transaction in which the Service User is the beneficiary of the transaction, including but not limited to receipt of a remittance transaction.

Article 11

Paragraph (1)

"Third party" is defined as any party comprising a reporting party as referred to in the laws and regulations concerning prevention and eradication of money laundering. CDD activities that may be performed by third parties are identification and verification of Service Users and Beneficial Owners, if any.

If when performing CDD, the Provider collaborates with another party not comprising a reporting party, the performance of CDD activities by that other party shall be deemed part of the performance of CDD by the Provider itself. The Provider shall bear full responsibility for the performance of CDD by that other party and shall ensure its compliance with the applicable regulations.

Paragraph (2)

Letter a

The scope of the CDD procedure includes but is not limited to identification and verification of prospective Service Users.

Letter b

Self-explanatory.

Letter c

This information shall at the least comprise information on the full name as stated on the identity card, address or place and date of birth, identity card number and nationality of the prospective Service User.

Letter d

The adequacy or otherwise of a nation's implementation of the FATF recommendations, among others, can be seen on the www.fatf-gafi.org or www.apgml.org websites.

Paragraph (3)

Ultimate responsibility for the results of identification and verification and the decision to engage in business dealings with a Service User shall be borne solely by the Provider.

Paragraph (4)

Self-explanatory.

Article 12

Letter a

Classification of high risk Service Users, among others, shall be guided by categories of Services Users with potential to commit Money Laundering and/or the guidelines established by PPATK concerning high risk Service Users.

Letter b

Self-explanatory.

Letter c

The amount of the transaction shall refer to Act No. 8 of 2010 concerning Prevention and Eradication of Money Laundering.

Article 13

Paragraph (1)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

"Transaction" is defined as including an application to become a CBPI holder, Electronic Money holder and order to execute a remittance.

Letter e

Self-explanatory.

Paragraph (2)

"Receipt transactions" are defined as transactions in which the Service user is the beneficiary in the transaction, including but not limited to receipt of remittance transactions.

Paragraph (3)

Self-explanatory.

Article 14

Paragraph (1)

Letter a

Document bearing information on the name and incorporation of a business Service User includes but is not limited to deed of incorporation or articles of association of the Service User. For Service Users comprising government/state institutions, it is sufficient for the documents to be presented to state the name and address of the government/state institution.

Letter b

Identity of management encompasses at least the name and address of the management of the Service User.

Letter c

Self-explanatory.

Letter d

Other legal documents may comprise the articles of association or internal rules of a Service User that constitute the basis of power to represent the Service User.

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Letter g

"Transaction" is defined as including an application to become a CBPI holder, Electronic Money holder and order to execute a remittance or funds transfer.

Letter h

Self-explanatory.

Paragraph (2)

"Receipt transactions" are defined as transactions in which the Service user is the beneficiary in the transaction, including but not limited to receipt of remittance transactions.

Paragraph (3)

Self-explanatory.

Article 15

Classification of high risk Service Users, among others, shall be guided by categories of Services Users with potential to commit Money Laundering and/or the guidelines established by PPATK concerning high risk Service Users.

"Senior officer" is defined as an officer of the Provider who has knowledge and experience concerning AML or PTF and has full powers at the Provider.

Article 16 …

Article 16

Direct responsibility is borne, among others, by the Board of Directors being directly involved in the AML and PTF processes for the these transactions for PEP Service Users, including but not limited to review and approval of EDD that has been performed on the Service User.

Article 17

Paragraph (1)

Self-explanatory.

Paragraph (2)

In the case of a Provider using the results of CDD performed by a third party, the face-to-face meeting may be conducted by the third party.

Article 18

Paragraph (1)

To support the document verification process, the Provider may demand other kinds of supporting documents bearing a recent identifying photograph of the Service User and/or prospective Service User within a period of remaining validity.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Provision of more than one identity document may be satisfied, for example, with the provision of an Identity Card and Driving Licence.

Paragraph (4)

Self-explanatory.

Article 19

Paragraph (1)

Self-explanatory.

Paragraph (2)

In monitoring, the Provider may set limits on amounts and types of transactions that deviate from the profile.

Paragraph (3)

Examples of transactions of high complexity include but are not limited to multiple transactions sent by several persons on behalf of the same person and multiple transactions sent by the same one person on behalf of several persons.

Article 20

Paragraph (1)

Self-explanatory.

Paragraph (2)

Identification and verification of a Beneficial Owner is performed using credible sources of data, including Articles of Association validated by the Ministry of Law and Human Rights and/or shareholder register.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 21

If the Provider discovers that a Service User is acting on behalf of a statutory/government institution or a company listed on the stock exchange, it is sufficient for the Provider to record the identity of the Beneficial Owner.

"Statutory/government institution" is defined as an institution vested with powers in the legislative, executive and judicial fields.

Article 22

Paragraph (1)

Documents may be administered in the form of originals, copies, in electronic form, microfilm or documents admissible as evidence under Law.

Letter a

The administered documents encompass at least the identity of the Service User, prospective Service User and/or Beneficial Owner and the transaction information. Transaction information includes but is not limited to transaction date, type and value of transaction, currency used, source of funds and purpose of transaction.

Letter b

Financial documents consist of records, bookkeeping evidence and supporting data for financial administration, which constitute evidence of the rights and obligations and the line of business of the Provider.

Paragraph (2)

In the event that the findings are classified as a Suspicious Transaction Report, the Provider shall forward the report to PPATK as referred to in Part Six.

Article 23

Self-explanatory.

Article 24

Paragraph (1)

Self-explanatory.

Paragraph (2)

Information used to establish a Service User profile includes but is not limited to information on the identity of the Service User and transactions performed, including the purpose of conducting transactions and source of funds if required.

Article 25

Self-explanatory.

Article 26

Paragraph (1)

Letter a

"Valid identity document" is defined as an Identity Card, Driving Licence, Passport or other identity document bearing at least a photograph and signature, issued by a competent authority and with remaining validity.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Paragraph (2) …

Paragraph (2)

Self-explanatory.

Article 27

Self-explanatory.

Article 28

"Sending Service User" is defined as the Service User issuing a funds transfer order in the first instance.

In conducting funds transfer activities, a Provider may act as sending Provider, forwarding Provider or beneficiary Provider. The sending Provider is the Provider sending the funds transfer order. The forwarding Provider is the Provider forwarding the funds transfer order. The beneficiary Provider is the Provider with the obligation to convey the funds to the Service User duly entitled to receive the funds.

Information on the identity of a sending Service User shall include at least the following:

a. name; and
b. account number, other unique reference number, address, identity number or information on place and date of birth.

Article 29

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

The provisions issued by PPATK include but are not limited to periods for submission of reports.

Article 30

Paragraph (1)

Self-explanatory.

Paragraph (2)

The audit function must possess capacity and knowledge pertaining to AML and PTF.

Paragraph (3)

Self-explanatory.

Article 31

It is also possible that employees of the payment system services provider itself are involved in exploitation of payment system services as a medium for money laundering and terrorism financing. Thus, to prevent or to detect actions suspected as money laundering through the provision of payment system services, it is necessary to implement Know Your Employee (KYE), among others conducted with a screening procedure.

Article 32

Self-explanatory.

Article 33

Paragraph (1)

Establishment of a dedicated unit and/or appointment of an officer shall take into consideration the needs and complexity of the payment system services operated by the Provider.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Adequate capacity includes but is not limited to experience and knowledge of developments in the AML and PTF regime.

Paragraph (4)

Self-explanatory.

Article 34

Paragraph (1)

"Relevant laws and regulations" are defined as including but not limited to the Act governing the prevention and eradication of money laundering.

Paragraph (2)

Self-explanatory.

Article 35

Self-explanatory.

Article 36

Self-explanatory.

Article 37

Letter a

Self-explanatory.

Letter b

"Line of business" is defined as activities in CBPI, Electronic Money or RS.

Letter c

"Licence" is defined as the licence of a Provider to conduct activities in CBPI, Electronic Money or RS.

Cancellation is the cancellation of a licence issued by Bank Indonesia to a Provider that has not opened for business.

Letter d …

Letter d

Revocation is the cancellation of a licence issued by Bank Indonesia to a Provider that has opened for business.

Article 38

"Licence" is defined as the licence of the Provider to conduct activities in CBPI, Electronic Money or RS.

Article 39

Self-explanatory.

Article 40

Self-explanatory.

Article 41

Self-explanatory.

SUPPLEMENT TO THE STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER 5302